UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,504	11/26/2003	Franck Le	60282.00102	6168

32294 7590 12/06/2007

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
12/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,504	LE ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/26/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 11/26/2003.

DETAILED ACTION

Claims 1-41 have been examined.

Title

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Priority

This application claims priority to Provisional Application 60/482,763, filed on 6/27/2003.

Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 6/27/2003.

Information Disclosure Statement

The information disclosure statement(s) (IDS) submitted on 11/26/2003 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements. However, the examiner notes, as indicated on the signed copy, that the references listed in the IDS did not properly identify the pertinent pages of each reference, and as such were not considered.

Drawings

The drawings filed on 11/26/2003 are acceptable for examination proceedings.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed

150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because:

The abstract contains multiple phrases which can be implied, such as “a method for”, "is provided”, “according to one embodiment”, “the method includes the steps of”, etc. The examiner further recommends that the abstract provide description of the types of information which may be required for performing the validity check, and description regarding the intermediate nodes, as this would aid a person reading the abstract in understanding the heart of the invention.

Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because it contains a plurality of embedded hyperlinks and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01. Appropriate correction is required.

The examiner further notes the applicants’ usage of the language “all necessary information required for performing a validity check” in the claims and throughout the specification. In order to remain consistent with the specification, the examiner has interpreted the usage of this language, for the purposes of searching and applying prior art, as meaning “all necessary information required for performing a validity check **without the checking entity needing to further communicate with the sending network node**". This interpretation is

consistent with the specification, as the specification clearly shows that the checking node does not require further communication with the sending node in order to perform the validity checking, but that the checking entity may need to receive additional information from somewhere (i.e. a certificate authority) in order to perform the validity checking.

Claim Objections

For the applicants' future reference:

A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claims 15-17, and 32 are objected to under 37 CFR 1.75, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 15 and 32, "the Public Key" lacks antecedent basis in the claims, and further should not be capitalized.

Regarding claim 16 and 17, the lack of punctuation renders the claim unclear as to what is performing the validity check. The examiner suggests the following "performing a validity

check, in a receiving node, of a packet by referring to the validity information contained in the header of the packet", for example.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5-10, 15-21, 23-26, 32, 34, 36, 37, 40, and 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Gupta et al. (US Patent Number 6,389,532) hereinafter referred to as Gupta.

Regarding claim 1, Gupta disclosed a method for protecting packets to be sent from a first network node (See Gupta Fig. 1 Element 108) to a second network node (See Gupta Fig. 1 Element 104 or 112), comprising the steps of: generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4), wherein the validity information comprises all necessary information required for performing a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); generating a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and sending the packet including the header from a first network node to a second network node (See Gupta Col. 6 Paragraph 4).

Regarding claim 18, Gupta disclosed a network node for sending packets (See Gupta Fig.

1 Element 108) to a receiving network node (See Gupta Fig. 1 Element 104 or 112), comprising:
2 first generating means for generating validity information for a packet (See Gupta Figs. 5-6 and
3 Col. 6 Paragraphs 2-4); second generating means for generating a header for the packet,
4 comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and sending
5 means for sending the packet including the header to a receiving network node (See Gupta Col. 6
6 Paragraph 4), wherein the validity information comprises all necessary information required for
7 performing a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7
8 Paragraph 2).

9 Regarding claim 19, Gupta disclosed a network node (See Gupta Fig. 1 Element 104 or
10 112) comprising: receiving means for receiving packets from a sending network node (See Gupta
11 Fig. 1 Element 108) (See Gupta Fig. 7 and Col. 6 Paragraph 5); and performing means for
12 performing a validity check of a packet by referring to validity information contained in a header
13 of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information
14 comprises all necessary information required for performing the validity check of the packet (See
15 Gupta Fig. 7 and Col. 6 Paragraph 5).

16 Regarding claim 20, Gupta disclosed a network node (See Gupta Fig. 1 Element 104)
17 comprising: forwarding means for forwarding packets from a sending network node to a
18 receiving network node (See Gupta Fig. 7 and Col. 7 Paragraph 2); and performing means for
19 performing a validity check of a packet by referring to validity information contained in a header
20 of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information
21 comprises all necessary information required for performing a validity check of the packet (See
22 Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2).

Regarding claim 34, Gupta disclosed a network system (See Gupta Fig. 1) comprising: a first network node (See Gupta Fig. 1 Element 108) configured to send a packet, wherein the first network node comprises first generating means for generating validity information for a packet (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4), second generating means for generating a header for the packet, comprising the validity information (See Gupta Col. 6 Paragraph 4); sending means for sending the packet including the header to a receiving network node (See Gupta Fig. 1 Element 104 or 112) (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required for performing a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); and a second network node configured to receive the packet (See Gupta Fig. 1 Element 104 or 112), wherein the second network node comprises performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2).

Regarding claims 2, 21, 36, and 37, Gupta disclosed that the step of generating the validity information comprises generating security information indicating security services applied to the packet (See Gupta Col. 5 Paragraph 7).

Regarding claim 3, Gupta disclosed that the step of generating the validity information comprises generating algorithm information to be used for performing the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4).

Regarding claim 5, Gupta disclosed that the step of generating the algorithm information comprises generating the algorithm information which comprises values to initialize an

algorithm to be used for performing the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example).

Regarding claims 6, 23, 40, and 41, Gupta disclosed that the step of generating the validity information comprises generating public key information of a sending node (See Gupta Col. 6 Paragraphs 2-6, for example the public and private key pair, or the key index).

Regarding claims 7 and 24, Gupta disclosed that the step of generating the public key information comprises generating reference information related to how a public key can be obtained (See Gupta Col. 6 Paragraphs 3-4 and Col. 7 Paragraph 2).

Regarding claims 8 and 25, Gupta disclosed that the step of generating the reference information comprises generating an identity of an entity from which the public key can be obtained (See Gupta Col. 6 Paragraphs 3-4, Col. 7 Paragraph 2, and Col. 3 Line 64 – Col. 4 Line 13, wherein the index is the identity, and the entry in the table is the entity).

Regarding claims 9 and 26, Gupta disclosed that the step of generating the reference information comprises generating a public key identifier for the public key (See Gupta Col. 6 Paragraphs 3-4 and Col. 7 Paragraph 2, the key index).

Regarding claim 10, Gupta disclosed that the step of generating the public key information comprises generating the public key (See Gupta Col. 6 Paragraph 2).

Regarding claims 15 and 32, Gupta disclosed signing the packet using a private key corresponding to the Public Key indicated by the validity information in the packet header in a sending network node (See Gupta Col. 6 Paragraph 4).

Regarding claim 16, Gupta disclosed performing a validity check of the packet by referring to the validity information contained in the header of the packet in a receiving node (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2).

Regarding claim 17, Gupta disclosed performing a validity check of a packet by referring to the validity information contained in the header of the packet in an intermediate node (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 33 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta.

Regarding claim 33, Gupta disclosed sending IP packets from a sender to a receiver through a network, but failed to specifically disclose that the sender could be a mobile network node. However, it was well known in the art at the time of application that packets senders could be mobile nodes such as laptops, PDAs, telephones, etc., and as such, in order to allow a user mobility of access to a network, it would have been obvious to the ordinary person skilled in the art at the time of invention to have incorporated a mobile node as a sender in the system of Gupta.

Regarding claim 35, Gupta disclosed validating packets at a recipient (router) but failed to specifically disclose validating the packets at the end recipient as well. However, it would have been obvious to the ordinary person skilled in the art at the time of invention to have performed the packet validation at the recipient as well. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that the packet was properly transmitted from the router to the recipient without error or illicit modification.

Claims 12-14, and 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta as applied to claims 1, 18, 19, and 20 above, and further in view of Naudus (US Patent Number 6,202,081).

Regarding claims 12-14, and 29-31, Gupta disclosed validation of packets, but failed to disclose that the step of generating the validity information comprises generating an information item for preventing replay attacks.

Naudus teaches that in a packet filtering system, packets should include timestamps in order to prevent replay attacks. Naudus further teaches that "[r]eplay attacks occur when a malicious user gains access to a router or other network device on a computer network that is forwarding data packets. Legitimate data packets are intercepted and then re-sent at a later time to allow the malicious user to appear as a legitimate user. A firewall helps prevent replay attacks by checking a time-stamp in the data packet that prevents the data packets from being re-sent at a later time." (See Naudus Col. 2 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Naudus in the packet validity checking system of Gupta by including a timestamp in each packet and verifying the timestamp at the validity checker. This

would have been obvious because the ordinary person skilled in the art would have been motivated to prevent replay attacks in the network. In this combination, the inclusion of a timestamp in each packet, in itself, is an indication of a procedure to be used for anti replay attacks.

Regarding claims 4, 22, 38, and 39, Gupta did not specifically teach that the step of generating the algorithm information comprises generating the algorithm information which indicates an algorithm to be used for performing the validity check of the packet. However, as taught by Naudus, in Col. 6 Line 60 - Col. 7 Line 7, it is well known to include in the packet header, an identification of which algorithm was used to sign the packet. As such, it would have been obvious to have included this information within the packet. Furthermore, the ordinary person skilled in the art at the time of invention would have recognized that this would allow for the user of a multiplicity of signature algorithms, as well as allowing updating of the signature algorithms in the future, and therefore it would have been obvious to have included an indication of the signature algorithm in the packet.

Claims 11, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta as applied to claims 6 and 23 above, and further in view of Nikander (US Patent Number 7,155,500).

Gupta disclosed including public key information within the packets, but failed to specifically disclose including the public key itself within the packets or that the step of generating the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

Gupta did disclose that the public and private key pairs can be generated and stored in a certification server (See Col. 4 Paragraph 2).

Nikander teaches that by including a public key itself and the certificate of the public key, the receiving host can verify that the public key is truly owned by the sender (See Nikander Col. 10 Line 50 – Col. 12 Line 9).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Nikander in the packet verification system of Gupta by including the public key and public key certificate within each packet and verifying that the sender of each packet owned the public key used to sign the packet. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that a malicious node was not claiming to be a different node.

Conclusion

Claims 1-41 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew Henning/
Assistant Examiner
Art Unit 2131
11/21/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100